

0- 793842

На правах рукописи



Строкачева Ольга Александровна

**ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ АНАЛИЗА ЗАЩИЩЕННОСТИ
ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ
ЭЛЕКТРОННОЙ КОММЕРЦИИ**

Специальность 08.00.13 – математические и инструментальные методы
экономики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата экономических наук

Ростов-на-Дону - 2008

2 12 ~~52/01-1272~~
08

Работа выполнена в ГОУВПО Ростовский государственный
экономический университет «РИНХ».

Научный руководитель: доктор экономических наук, доцент
Тищенко Евгений Николаевич

Официальные оппоненты: доктор экономических наук, профессор
Долятовский Валерий Анастасьевич

кандидат технических наук, доцент
Серпенинов Олег Витальевич

Ведущая организация: ГОУ ВПО «Южный федеральный
университет»

Защита состоится «22» декабря 2008 года в 13³⁰ часов на заседании
диссертационного совета ДМ 212.209.03 в Ростовском государственном
экономическом университете «РИНХ» по адресу: 344002, г. Ростов-на-Дону,
ул. Большая Садовая, 69, ауд. 231.

С диссертацией можно ознакомиться в научной библиотеке Ростовского
государственного экономического университета «РИНХ»

Автореферат разослан «21» ноября 2008 года.

Ученый секретарь
диссертационного совета



И.Ю. Шполянская

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

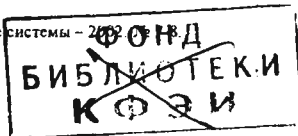
Актуальность темы исследования. Рост глобальной сети Интернет и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. К числу наиболее перспективных направлений относится бизнес с использованием новых информационно-технологических возможностей, которые облегчают распространение информации, повышают эффективность производственных процессов. Под электронной коммерцией понимается технология, обеспечивающая полный замкнутый цикл операций, включающий заказ товара (услуги), проведение платежей, участие в управлении доставкой товара (выполнения услуги). Эти операции проводятся с использованием электронных средств и информационных технологий и обеспечивают передачу прав собственности или прав пользования одним юридическим (физическим) лицом другому¹.

Одним из важнейших условий существования электронной коммерции является информационная безопасность, под которой понимается защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации. Ущерб от нарушения информационной безопасности может привести к крупным финансовым потерям².

Объективно оценить текущее состояние информационной безопасности компании, а так же ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности компании есть основные задачи аудита информационной безопасности. Поэтому под термином «анализ защищенности экономических информационных систем электронной коммерции» будем понимать

¹ Волокитина А.В. «Электронная коммерция» под ред. Реймана Л.Д. – М.: НТИ «ФИОРД-ИНФО», 2002. – 272 с.

² Астахов А. Анализ защищенности корпоративных систем // открытые системы – 2002. № 11.



системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности экономической системы в соответствии с определенными критериями и показателями безопасности³.

Многообразие представленных на рынке средств и методов анализа защищенности экономических информационных систем электронной коммерции (ЭИСЭК), отсутствие математической основы и научного базиса позволило сделать вывод об актуальности исследуемого вопроса.

Степень разработанности проблемы. Большое внимание в настоящее время уделяется проблемам оценки защищенности корпоративных систем Интернет/Инtranет. Эта предметная область рассматривается в работах ученых и специалистов-практиков С.А.Петренко, А.А. Петренко, А. Астахова, Е.Н Тищенко, Д.В. Слярова, Маркуса Ранума и других.

Вопросам разработки и анализа характеристик информационных систем и моделирования бизнес-процессов посвящены работы Г.Н. Хубаева, К.Р. Адамадзиева, С.В. Баранова, Г. Буча, К. Дж. Дейта, А. Джекобсона, А.А. Емельянова, Е.Н. Ефимова, С.В. Ивахненко, Э. Кармайкла, Г. Майерса, Б. Мейера, Э. Нейбурга, Дж. Рамбо, Д. Хейвуда, А. Элиенса и других.

Однако, несмотря на большое внимание, уделяемое данной предметной области, не было обнаружено исследований, посвященных классификации программных продуктов для анализа защищенности корпоративных систем Интернет/Инtranет. Кроме того, мало внимания уделено применению данных программных продуктов в области оценки защищенности ЭИСЭК. Этими обстоятельствами обусловлен выбор темы диссертационного исследования.

Объектом исследования являются предприятия всех организационно-правовых форм собственности и отраслей экономики, деятельность которых связана с использованием ЭИСЭК.

Предметом исследования являются процессы обеспечения защищенности ЭИСЭК.

³ Петренко С.А., Петренко А.А. Аудит безопасности Internet. – М.: ДМК Пресс, 2002.

Цель и задачи диссертационного исследования. Основной целью диссертационного исследования является развитие инструментария анализа защищенности ЭИСЭК.

Поставленная в работе цель обусловила решение следующих научных проблем и практических задач:

- классификация программных средств анализа защищенности ЭИСЭК;
- разработка методики анализа защищенности ЭИСЭК;
- разработка программного инструмента для анализа защищенности ЭИСЭК.

Теоретическая база исследования. Теоретической и методологической основой исследования являются труды отечественных и зарубежных ученых по теории экономических информационных систем и информационной безопасности, законодательные и нормативные акты в области электронной коммерции, инструктивные материалы, материалы научных конференций, публикации в периодической печати.

Работа выполнена в рамках пункта Паспорта специальности 08.00.13 – математические и инструментальные методы экономики: 2.6. «Развитие теоретических основ методологии и инструментария проектирования, разработки и сопровождения информационных систем субъектов экономической деятельности: методы формализованного представления предметной области, программные средства, базы данных, корпоративные хранилища данных, базы знаний, коммуникационные технологии».

Эмпирической базой исследования явились экспериментальные и статистические данные собранные в процессе эксплуатации ЭИСЭК ряда организаций. Основные выдвигаемые научные положения и рекомендации экспериментально подтверждены.

Инструментарий исследования составил классические методы анализа защищенности распределенных экономических информационных систем, метод групповых экспертных оценок, методы сравнения программных систем по критерию функциональной полноты, методы

целочисленного программирования а так же программные средства общего и специального назначения.

Научная новизна диссертационного исследования заключается в разработке целостного инструментального обеспечения для экономико-математического анализа защищенности ЭИСЭК. Научную новизну содержат следующие основные результаты:

1. Разработана отсутствующая на сегодняшний день классификация программных средств анализа защищенности экономических информационных систем, учитывающая особенности систем электронной коммерции. Данная классификация систематизирует инструментальные средства анализа защищенности по двум группам:

- системы комплексного внешнего аудита экономических информационных систем информационной безопасности организации на основе международных стандартов в области защиты информации;

- системы автоматизированного анализа защищенности экономических информационных систем, позволяющие дать объективную оценку состояния информационной безопасности на основе исследования топологии распределенной информационной системы организации.

2. Сформирован наиболее полный на сегодняшний день перечень требований, предъявляемых к функциональным характеристикам экономических информационных систем в области электронной коммерции, позволяющий провести оценку качества существующих программных средств в соответствии с разработанной классификацией. Данный перечень включает в себя основные функциональные характеристики, которым должны отвечать инструментальные средства анализа защищенности экономических информационных систем электронной коммерции.

3. Разработана математическая модель анализа защищенности ЭИСЭК, основывающаяся на сигнатурном и статистическом методах. Данная модель позволяет проводить анализ систем ЭК на наличия в них возможных совокупностей угроз.

4. Предложена модель комплексного анализа защищенности ЭИСЭК на основе последовательности атакующих элементарных операций. Данная модель позволяет определять вероятность вскрытия защитных механизмов за заданное время.

Практическая значимость результатов исследования состоит в том, что основные положения, выводы. Рекомендации, модели, методы и алгоритмы могут быть использованы предприятиями и организациями любой структуры ведомственной принадлежности и формы собственности для оценки защищенности ЭИСЭК.

Апробация и внедрение результатов исследования. Основные результаты диссертационной работы докладывались и обсуждались на Международных и Всероссийских конференциях, в том числе: VIII Международная научно-практическая конференция «Экономико-организационные проблемы проектирования и применения информационных систем» (Кисловодск, 27-29 октября 2005г.); Международная научно-практическая конференция «Проблемы информационной безопасности» (Ростов-на-Дону, 22 ноября 2005г.); Региональная научно-практическая конференция молодых ученых и специалистов «Высокие информационные технологии» (Ростов-на-Дону, 20 апреля 2005г.); VIII Международная научно-практическая конференция «Информационная безопасность» (Таганрог, 3-7 июля 2006г.); Шестая международная конференция «Информационные технологии и безопасность-2006» (Партенит (Крым, Украина) 19-23 октября 2006г.); Всероссийская научно-практическая Интернет-конференция «Проблемы информационной безопасности» (Ростов-на-Дону, 20-27 ноября 2006г.); Межвузовская научно-практическая конференция «Статистика в современном мире: методы, модели, инструменты: материалы» (Ростов-на-Дону, 26 апреля 2007г.); Вторая Всероссийская научно-практическая Интернет-конференция «Проблемы информационной безопасности» (Ростов-на-Дону, 14-18 мая 2007г.); IX Международная научно-практическая конференция «Информационная безопасность» (Таганрог, 3-7 июля 2006г.);

IX Международная научно-практическая конференция «Экономико-организационные проблемы проектирования и применения информационных систем» (Кисловодск, 22 декабря 2007г.); так же доклад «Построение имитационной модели для анализа защищенности систем электронной коммерции» был заслушан в финале Седьмого Всероссийского конкурса студентов и аспирантов по информационной безопасности «SIBINFO-2007» (Томск, 18 апреля 2007г.)

Основные положения полученные в результате проведенного исследования используются при чтении курса «Информационная безопасность в системах электронной коммерции», специальности «Организация и технология защиты информации».

Отдельные результаты диссертационной работы использованы при анализе защищенности ЭИСЭК в образовательной деятельности (РГЭУ «РИНХ»), в бизнес структурах (ООО «ФОТО-ЛЭНД», ООО «Топ-книга») и на предприятиях иных видов деятельности. Результаты исследования использованы в типовом программном обеспечении «Advanced Security Test» (свидетельство о государственной регистрации программы для ЭВМ № 2008610753). Также отдельные направления представленного научного исследования реализовывались в рамках гранта РГЭУ «РИНХ» «Инструментальные методы создания и анализа качества защищенной среды функционирования информационных систем». Документы, подтверждающие внедрение, прилагаются к диссертации.

Публикации. По результатам диссертационного исследования опубликовано 17 печатных работ, 3 из которых рекомендованы ВАК, общим объемом 3,14 п.л.

Структура и объем работы. Диссертационная работа состоит из введения, трех глав, заключения, библиографического списка и приложений. Работа содержит 96 страниц основного текста, 29 страниц приложений, 13 рисунков, 12 таблиц, библиографический список включает 105 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

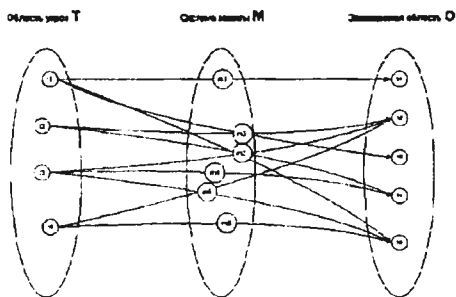
Во введении обоснована актуальность темы диссертационного исследования, сформулированы цели и задачи исследования, определены объект, предмет и методы исследования, приведены элементы научной новизны и положения, выносимые на защиту.

В первой главе «Анализ защищенности систем электронной коммерции» построена модель защиты информации с полным перекрытием для экономических информационных систем ЭК. Рассчитаны вероятности интенсивности атак, реализуемых в течении заданных временных промежутков. Рассчитаны экономические потери при реализации угроз на исследуемые системы ЭК.

Выявлен ранжированный список критериев качества системы ЭК, показывающий уровень защищенности систем ЭК в целом. Осуществлено тестирование системы защиты в соответствии с данным списком. Построена модель для оценки защищенности экономических информационных систем ЭК.

На основе анализа существующей нормативной базы в области информационной безопасности был сформирован наиболее полный перечень документов и нормативных актов, регламентирующих построение и аудит системы защиты экономических информационных систем ЭК.

Так как основой формального описания систем защиты традиционно считается модель системы защиты экономических информационных систем мы построили модель системы защиты с полным перекрытием для систем, ЭК, в которой рассматривается взаимодействие «области угроз», «защищаемой области» (ресурсов информационной системы) и «системы защиты» (механизмов, обеспечивающих безопасное функционирование информационной системе) (см. рис. 1).

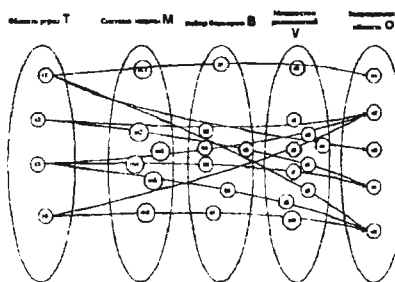


Источник: авторская

модификация графа из работы Хоффман Л. Дж. «Современные методы защиты информации», 1980

Рисунок 1- Графовая модель системы защиты с полным перекрытием

Исследуя модель, мы вводим в нее перечень уязвимостей и анализируем следующую модификацию модели Хоффмана (см. рис. 2):



Источник: авторская модификация графа из работы Хоффман Л. Дж. «Современные методы защиты информации», 1980

Рисунок 2 - Модель системы защиты, содержащая уязвимости

В системах с полным перекрытием для любой уязвимости имеется соответствующий барьер, устраняющий эту уязвимость.

Таким образом, в системе защиты с полным перекрытием для всех возможных угроз безопасности существуют механизмы защиты,

препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность ЭИСЭК. Исследование модели привело к формированию перечня критериев, позволяющих определить защищенность ЭИСЭК.

Для формирования этого списка был использован метод экспертных оценок, основанный на методе Дельфи, и определением расстояния Кемсни. В качестве экспертов были привлечены ведущие специалисты в области информационной безопасности, сфера интересов которых связана с системами электронной коммерции. На основе выделенных критериев было реализовано моделирование процесса тестирования реальных систем электронной коммерции. Так же нами был предложен алгоритм конфигурирования элементов системы защиты ЭИСЭК.

Таблица 1 – Результаты тестирования системы на ошибки

Типы ошибок	Вероятность появления	Количество ошибок при проведении испытания N_i
Ошибки вычислений	0,26	5
Логические ошибки	0,9	---
Ошибки ввода-вывода	0,8	4
Ошибки манипулирования данными	0,2	25
Ошибки сопряжения	0,17	11
Ошибки определения данных	0,08	3
Ошибки в БД	0,16	3

Источник: авторский

В результате тестирования получаем вероятность безотказной работы системы.

Зная общее количество часов корректной работы, мы можем оценить ресурсы, затрачиваемые на внедрение системы защиты, трудовые затраты на внедрение системы и т.д.

Таблица 2 – Исходные данные для решения задачи

№	Инструменты защиты	I_z (количество защитных механизмов)	H (часы)
1	CheckPoint FW-1	712	510
2	Cisco Pix Firewall	620	452
3	Gauntlet Firewall	513	436
4	Symantec Raptor Firewall	650	520
5	Secure Computing's Sidewinder Firewall	410	380
6	Watch Guard Appliance Firewalls	530	461
7	Snot IDS	230	190
8	Shadow IDS	350	293
9	PortSentry IDS	510	471
10	Tripwire IDS	438	356
11	RealSecure Network Sensor IDS	573	478
12	Symantec Enterprise Security Manager (ESM)	712	602
13	E-Security Open e-Security Platform	560	408
14	Tivoli Net View	329	260

Источник: авторский

На сегодняшний день нет четко обозначенной нормативной базы обеспечения защищенности систем электронной коммерции. Есть большое количество законов и нормативных документов разного уровня. Это законы, стандарты, другие нормативные документы ВСТЕК, ФСБ, отраслевых министерств, которые определяют общие принципы функционирования информационных систем.

Во второй главе «Методы формализованного анализа уровня защищенности экономических информационных систем» были исследованы инструментальные средства анализа защищенности ЭИСЭК. В результате были выявлены схожие по набору функций инструменты анализа защищенности ЭИСЭК. Исследование показало отсутствие реализации функций анализа защищенности ЭИСЭК в существующих инструментальных средствах.

Далее был сформирован перечень операций, обеспечивающий наиболее полное на сегодняшний день исследование систем ЭК. Исследование показало отсутствие у анализируемых систем требуемого перечня функциональных операций, что позволило сделать вывод о необходимости

разработки методики и реализации инструментария, позволяющего исследовать защищенности систем электронной коммерции, с учетом специфической реализации подобных технологий.

Основным инструментарием анализа защищенности ЭИСЭК является большое количество (около 17) программно-аппаратных комплексов, соответствующих исследуемой области.

Исследование показало, что все эти средства условно можно разделить на две группы: полностью автоматизированный средства анализа защищенности экономических информационных систем или средства, основанные на частичной автоматизации или интерактивном человеко-машинном диалоге, позволяющим сформулировать степень защищенности экономической информационной системы в целом (см. рис. 3).

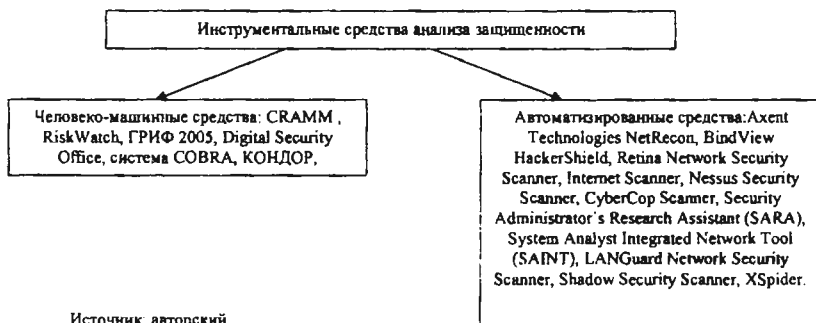


Рисунок 3 –Инструментальные средства анализа защищенности

Также в диссертационном исследовании был сформирован наиболее полный перечень на сегодняшний день функциональных операций и на его базе был осуществлен сравнительный анализ ведущих коммерческих систем, приведенных на рисунке 3, с использованием формального анализа⁴. Исследование показало, что существующие системы анализа защищенности

⁴ Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты// Программные продукты и системы (SOFTWARE&SYSTEMS).–1998.–N2.

Далее была исследована структура и логика работы существующих систем анализа защищенности ЭИСЭК и обобщены в виде схемы на рисунке4.

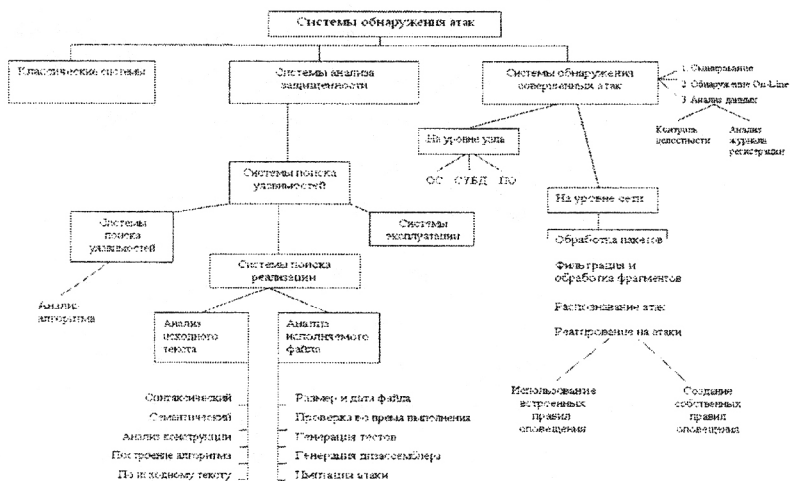


Рисунок 4 – Структура и логика работы систем анализа защищенности

На основе анализа и модификации существующих методик ⁵⁶⁷⁸⁹ разработана модель анализа защищенности ЭИСЭК, представляющая собой следующий алгоритм:

14

1. Формирование матрицы статистических характеристик сетевого трафика;
2. Формирование матрицы сигнатурных характеристик сетевого трафика;
3. Сравнение матрицы сигнатурных характеристик трафика с эталонными базами стандартных атак;
4. На базе матрицы статистических характеристик определяется разность времени передачи пакета между реальным временем и эталонным временем;
5. Определяется наличие сигнатуры известной атаки или аномального трафика с превышением времени передачи пакета.

Необходимо заметить, что формальная модель аудита систем электронной коммерции, описанная таким образом, позволяет проводить анализ статистических и сигнатурных элементов, путем выявления в них возможных совокупностей рисков. Такая процедура осуществляется путем анализа рисков.

Заключительным этапом формального описания модели аудита систем ЭИСЭК является формализация процесса комплексного анализа защищенности и среды ЭК.

В соответствии с математической моделью схематически изобразить комплексный процесс анализа защищенности ЭИСЭК можно в виде блок-схемы состоящей из семи блоков, представленной на рисунке 5.

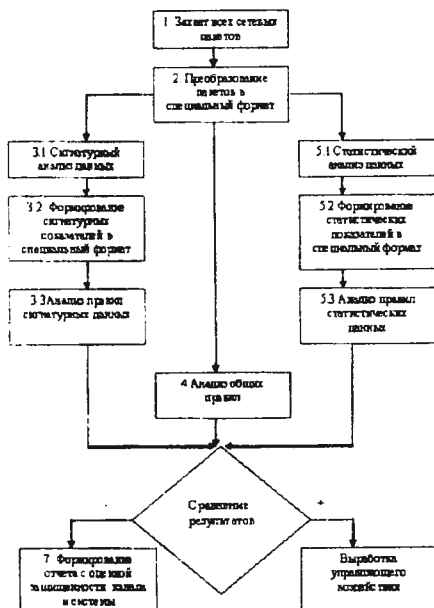
⁶ Математическая модель процессов связи узлов сети при обнаружении предотвращении несанкционированного доступа к информации / В.С. Пелешенко // Материалы 9-й региональной научно-технической конференции «Вузовская наука – северо-кавказскому региону». - 2005

⁷ В.П. Гергель, Р.Г. Стронгин Основы параллельных вычислений для многопроцессорных вычислительных систем: Учеб. пособ. издание 2-е, доп. - г.Нижний Новгород: изд-во Нижегород. гос. ун-та, - 2003.

⁸ http://www.software.unn.ru/cscam/files/HTML_Version/index.html#Contents

⁹ Тищенко Е.Н. Анализ защищенности экономических информационных систем: Монография – Ростов н/Д.: РГЭУ «РИНХ», 2003. - 192 с.

⁹ Перенко С.А., Петренко А.А. Аудит безопасности Internet. – М.: ДМК Пресс, 2002.

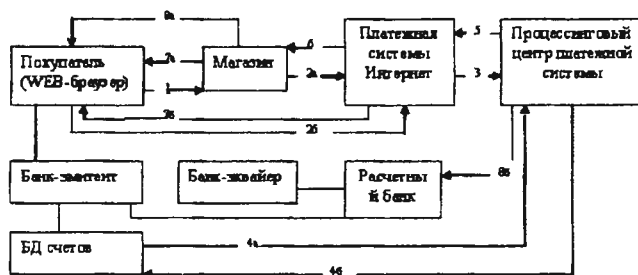


Источник: модифицированная схема А.Ф. Чипига, В.С. Пелешенко, Формализация процедур обнаружения и предотвращения сетевых атак/ Информационная противодействие угрозам терроризма. Научно-практический журнал №8-2006г.

Рисунок 5- Схема функционирования процесса анализа защищенности ЭИСЭК

В третьей главе «Оценка эффективности модели анализа защищенности экономических информационных систем электронной коммерции» на основе математической модели, описывающей алгоритм анализа защищенности ЭИСЭК была построена имитационная модель анализа защищенности систем электронной коммерции.

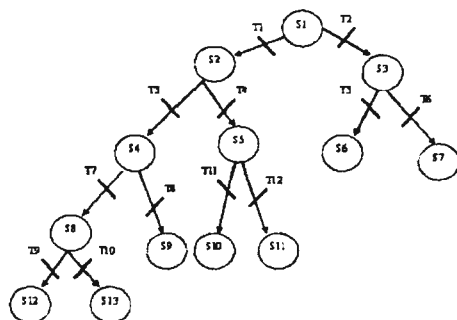
Была сформирована общая схема функционирования ЭИСЭК, включающая в себя весь цикл функциональных операций (см. рис. 6).



Источник: модифицированная схема, приведенная в www.e-commerce.ru

Рисунок 6 - Схема комплексной интегрированной среды электронной коммерции

В соответствии с данной схемой на основе сетей Петри был промоделирован процесс атак на ЭИСЭК с использованием элементарных атакующих операций (см. рис. 7).



Источник: авторский

Рисунок 7- Графическая модель возможных атак на ЭИСЭК

Далее была произведена оценка разработанной модели анализа угроз для ЭИСЭК с использованием инструментально-моделирующего комплекса оценки качества функционирования информационных систем «КОК»¹⁰. Аудит систем ЭИСЭК производится методом постоянного мониторинга ресурсов

¹⁰ Безжоровый М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс оценки качества функционирования информационных систем «КОК»: Руководство системного аналитика. - М.: Вооружение. Политехника. Криверсия.2002.-305 с., 2-е издание

сети. Результатами оценки являются вероятности возникновения угроз на ЭИСЭК (см. рис. 8).



Источник: авторский

Рисунок 8 – Результаты расчетов нарушения целостности ЭИСЭК

В заключении диссертационной работы приведены основные выводы по результатам проведенного исследования.

По теме диссертации автором опубликованы следующие работы:

Статьи в периодических научных изданиях, рекомендованных ВАК РФ и свидетельство о государственной регистрации:

1. Тищенко Е.Н., Строкачева О.А. Модель аудита информационной безопасности систем электронной коммерции // Научная мысль Кавказа Северо-кавказский научный центр высшей школы, приложение № 14 (98) 2006. (подписано к печати 15.12.2006.). – с. 134-141 – 0,31 п.л., в т.ч. авторских 0,29 п.л.

2. Тищенко Е.Н., Строкачева О.А. Методика оценки рисков при проведении аудита систем электронной коммерции // Известия высших учебных заведений Северо-кавказском регион Технические науки. № 3 (139) 2007. (подписано к печати 14.05.2007.). - с. 139-142 – 0,32 п.л., в т.ч. авторских 0, 28 п.л.

3. Строкачева О.А. Построение модели анализа защищенности экономических информационных систем электронной коммерции // Экономические Науки Современный экономический журнал № 46 2008. – с. 387-393 - 0,34 п.л.

4. «Advanced Security Test» / Свидетельство о государственной регистрации программы для ЭВМ № 2008610753, Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (авторы: Е.Н. Тищенко, О.А. Строкачева, С.Ю. Миргородский). – М., 2008.

Статьи в сборниках научных трудов и материалов докладов конференций:

5. Тищенко Е.Н., Строкачева О.А. Критерии качества систем электронной коммерции // Проблемы федеральной и региональной экономики: Ученые записки. Вып. 9/ РГЭУ «РИНХ».- Ростов н/Д, 2006. – с. 95-99 – 0,2 п.л., в т.ч. авторских 0, 15 п.л.

6. Тищенко Е.Н., Строкачева О.А. Оценка параметров надежности защищенной платежной системы в электронной коммерции // Вестник Ростовского Государственного Экономического университета «РИНХ» №2 (22) 2006. – с. 115-123 – 0,43 п.л., в т.ч. авторских 0, 21 п.л.

7. Тищенко Е.Н., Строкачева О.А. Методы оценки защищенности программно - аппаратных составляющих систем электронной коммерции // Информационные технологии и безопасность. Сборник научных трудов. Вып.9/Институт проблем регистрации информации НАН Украины. –Киев, 2006. - с. 173-182 – 0,31 п.л., в т.ч. авторских 0, 27 п.л.

8. Строкачева О.А., Уваренков С.И. Проблемы информационной безопасности в электронных платежных системах // Информационные системы, экономика, управление трудом и производством: Ученые записки. Вып. 10/РГЭУ «РИНХ». – Ростов н/Д, 2006. – с. 53-57 – 0,21 п.л., в т.ч. авторских 0, 12 п.л.

9. Строкачева О.А. Анализ безопасности платежных систем в электронной коммерции // Вопросы экономики и права: Сборник научных статей аспирантов и соискателей. Вып. 4/РГЭУ «РИНХ». - Ростов н/Д, 2006. - с. 133-137 – 0,16 п.л.

10. Строкачева О.А., Миргородский С.Ю. Методы оценивания информационных рисков в среде корпоративной системы как сегмента Интернет//Проблемы информационной безопасности: Материалы всероссийской научно-практической Интернет-конференции/РГЭУ «РИНХ». - Ростов н/Д, 2006. –с. 33-37 – 0,17 п.л., в т.ч. авторских 0, 1 п.л.

11. Тищенко Е.Н., Строкачева О.А. Вероятностные методы анализа защищенности систем электронной коммерции // Материалы VIII Международной научно-практической конференции «Информационная безопасность»/Таганрог: Изд-во ТРТУ, 2006. - с. 204-207 – 0,17 п.л., в т.ч. авторских 0, 09 п.л.

12. Строкачева О.А. Формальное определение защищенности систем электронной коммерции // Экономические и социально-правовые проблемы России. Экономика и статистика: Сборник научных трудов. Ч.2/Под ред. Д-ра экономических наук Н.П. Масловой. - Ростов н/Д: РСЭИ, 2007. - с. 111-120 – 0,27 п.л.

13. Строкачева О.А. Анализ рисков при построении защищенной системы электронной коммерции // Проблемы информационной безопасности: Материалы второй всероссийской научно-практической Интернет-конференции профессорско-преподавательского состава. 14-18 мая 2007 года/РГЭУ «РИНХ». - Ростов н/Д, 2007. – с. 61-63 – 0,09 п.л.

14. Строкачева О.А. Построение модели с полным перекрытием для объекта электронной коммерции//Статистика в современном мире: методы, модели, инструменты: материалы межвузовской научно-

практической конференции/РГЭУ «РИНХ». - Ростов н/Д, 2007. – с. 149-151 – 0,19 п.л.

15. Тищенко Е.Н., Строкачева О.А. Проблематика оценки защищенности информационных ресурсов на примере систем электронной коммерции//Материалы IX Международной научно-практической конференции «Информационная безопасность»/Ч.2- Таганрог: Изд-во ТРТУ, 2007.- с. 186-191 – 0,37 п.л., в т.ч. авторских 0, 27 п.л.

16. Строкачева О.А. Построение имитационной модели для анализа защищенности систем электронной коммерции // Вопросы экономики и права: сборник научных статей аспирантов и соискателей ученой степени кандидата наук. Вып. 5/РГЭУ «РИНХ».- Ростов н/Д, 2007. - с. 152-156 – 0,19 п.л.

17. Тищенко Е.Н., Строкачева О.А., Кравченко А.А. Комплексная оценка защищенности систем электронной коммерции // Информационные системы, экономика, управление трудом и производством: Ученые записки. Вып. 11/РГЭУ «РИНХ». – Ростов н/Д, 2007. – с. 160-164 – 0,22 п.л., в т.ч. авторских 0, 12 п.л.

Изд. № 235/631. Подписано в печать 20.11.2008.
Печать цифровая. Бумага офсетная. Гарнитура «Times New Roman».
Формат 60х84/16. Объем 1,0 уч.-изд. л.
Тираж 120 экз. Заказ № 004276.

344006, Ростов-на-Дону, ул. Б. Садовая, 69, тел. 261-38-45
Отпечатано в КМЦ ООО«АИЗ ЛТД»

